ObjectSecurity® OpenPMF™

Model-Driven Security Policy Automation

Ulrich Lang, PhD
Co-Founder & CEO

Watch the presentation recording at: youtube.com/watch?v=bjnLj1VdifA
Overview

- **ObjectSecurity**: leader in model-driven security (MDS) policy automation (esp. for access control)
- **Problem**: Security policies are often:
  - either unmanageable, e.g. ABAC etc. or not good enough, e.g. IBAC/RBAC
- **Solution**: Model-driven security:
  - Automatically generate technical rules from human-intuitive, “undistorted” models
  - Automatically update technical rules when IT landscapes change
  - Automatically generate compliance/accreditation evidence
- **ObjectSecurity OpenPMF™**: leading, award-winning MDS product
  - (1) Reduces cost; (2) Improves security & accreditation/compliance; (3) Supports security for today's agile, interconnected applications (e.g. SOA/cloud).
Cyber Capabilities

- **Key threats / vulnerabilities mitigated.** We prevent/minimize:
  - Unauthorized access
  - Access overprovisioning (→ get least privilege)
  - Access control policy errors & management shortcomings
    - Especially for agile IT landscapes (SOA etc.)
  - Agile certification & accreditation turnaround time

- **Cyber gaps accommodated:** Model-driven security:
  - Access control that is both:
    - Fine-grained, contextual, dynamic, system/user/info-flow based
    - Manageable, human-intuitive, general, verifiable
ObjectSecurity

Company: The policy automation experts. Founded in 2000 by Dr. Ulrich Lang (CEO) and Rudolf Schreiner (CTO), offices: San Diego & SF + Cambridge, UK

Product: OpenPMF model-driven security policy automation (since 2003), 2 patent apps, award-winning, various large customers

Services & consulting/R&D: since 2000

Dr. Ulrich Lang

- Founder & CEO
- PhD University of Cambridge, “Access Policies for Middleware”
- Master’s Information Security
- Board of Cloud Security Alliance (CSA), Silicon Valley Chapter
- Book author, public speaker, technical expert witness etc.
“we generally favor ‘model driven security to actually execute and implement digital dynamic access control...’
“cool vendor in authentication & application security”
“thorough and enlightening”
“in-depth technical knowledge + industrial experience”
“rapid one-to-one support, highly knowledgeable”
“well-known security experts”
“significant experience in security management”
“leading SOA security & enterprise policy experts”
“highly competent, well-managed and cost-effective”
The Challenge

Unmanageable Security Policies: How author policies, maintain technical implementation, check correctness/compliance?

- Manually translating policy into effective technical implementation is difficult, expensive, and error-prone - esp. for interconnected, agile applications (e.g. SOA & cloud)
  - Where does the policy come from?
  - Who can write the matching technical policy rules?
  - Who can maintain them despite dynamic changes?
  - Who can verify policy correctness & compliance?

Business drivers: Reduce cost, improve IT security & compliance, support agility

Technical need: preventive policy enforcement

- Access control that is meaningful to the business,
- that is preventive ("whitelisting"), manageable, supports IT agility, is repeatable/traceable/verifiable
The Solution

OpenPMF™ Model-Driven Security (MDS)

Definition

- Tool supported process
- Model “undistorted” security requirements models at a high level of abstraction,
- Using other information sources available about the system (produced by other stakeholders, expressed in Domain Specific Languages, DSL),
- Transform models into enforceable security rules with as little human intervention as possible.
- Includes the run-time security management (e.g. entitlements / authorizations), i.e. run-time enforcement, dynamic policy updates, policy incident monitoring.

The Solution

OpenPMF™ Model-Driven Security (MDS)

- Makes application security manageable
- Automates the process of turning “undistorted”, generic, human-understandable security & compliance requirements into the matching numerous and ever-changing technical security policy rules (whitelists) and configurations.
- Supports least privilege and workflow policies, which can protect against insider attacks.
- Distributes and proactively enforces those rules (e.g. at the application layer) & monitors
- Simplifies policy management more than other approaches (e.g. visual/linguistic) or traditional manual authoring of rules
- Works even for agile IT landscapes (e.g. SOAs)
- Critical part of any ABAC/authorization management & IAM strategy
- Enables a secure application development lifecycle at development time right from the beginning – dealing with policy abstraction, externalization, authoring, automation, enforcement, audit monitoring/reporting, and verification.

Object Security
Secure technology

info@objectsecurity.com
www.objectsecurity.com
OpenPMF™ Model-Driven Security Policy Automation

Problem
Unmanageable Security Policies
Manually translating security policy & compliance requirements into effective technical implementation is difficult, expensive, and error-prone - esp. for interconnected, agile applications (e.g. SOA & Cloud). Where does the policy come from? Who can write the matching technical policy rules? Who can maintain them despite dynamic changes? Who can verify policy correctness & compliance?

Solution
OpenPMF™ Model-Driven Security (MDS)
OpenPMF makes application security manageable through MDS automation. MDS automates the process of turning human-understandable security & compliance requirements (e.g. for attribute-based access control, ABAC, and monitoring) into the matching numerous and ever-changing technical security policy rules (whitelists) and configurations. MDS also distributes and proactively enforces those rules at the application layer, and also continuously monitors security. Unlike traditional manual authoring of rules, MDS automates technical policy generation and update from intuitive business security requirements models - including least privilege and workflow policies, which can protect against insider attacks. MDS helps automate policy management even for agile SOAs and cloud platforms. MDS forms a critical part of any authorization management, entitlement management and identity & access management (IAM) strategy. MDS also enables a secure application development lifecycle at development time right from the beginning - dealing with policy abstraction, externalization, authoring, automation, enforcement, audit monitoring/reporting, and verification.

1 Configure
intuitive business security requirements policies
Security professionals can configure or select generic application security requirements in a model-driven security tool, including access and monitoring policies. No need to be an application specialist.

2 Generate
matching technical security policies automatically
Application developers can implement application specific technical application security policy rules at the click of a button. Model-driven security automatically analyzes your software as it is being written or updated, and generates the matching fine-grained access and monitoring policies. No need to be a security specialist.

3 Enforce
technical security policies automatically
At runtime, local authorization management policy decision points and policy enforcement points (PDPs/PPEAs) underneath all applications automatically intercept and check all information flows before they are forwarded to the application.

4 Monitor
technical security policies automatically
At runtime, policy monitoring points automatically collect information about security incidents for monitoring and auditing purposes. The collected information can be configured through generic monitoring policy models.

5 Update
technical security policies automatically
Model-driven security uniquely updates technical security policies automatically when systems are reconfigured (e.g. SOA). No need to manually update technical security policies. This unique feature makes policy management and implementation manageable for today's rapidly evolving interconnected applications (e.g. agile SOA w. BPM and clouds).

6 Verify
compliance/accroutation automatically
This MDS feature automatically produces supporting evidence that the enforced security rules match with accreditation/compliance policy models and security policy models. It helps shorten accreditation/re-accreditation time and reduce cost (esp. for agile IT landscapes such as SOAs)

References objectsecurity.com/publish/
OpenPMF™: 1. Configure intuitive business security requirements policies

Security professionals can configure or select generic application security requirements in a model-driven security tool, including access and monitoring policies. No need to be an application specialist.
OpenPMF™: 2. Generate matching technical security policies automatically

Application developers can implement application specific technical application security policy rules at the click of a button. MDS automatically analyzes your IT landscape, and generates the matching fine-grained access and monitoring policies. No need to be a security specialist.
OpenPMF™: 3. Enforce technical security policies automatically

At runtime, local authorization management policy decision points and policy enforcement points (PDPs/PEPs) underneath all applications automatically intercept and check all information flows before they are forwarded to the application.
OpenPMF™: 4. Monitor technical security policies automatically

At runtime, policy monitoring points automatically collect information about security incidents for monitoring and auditing purposes. The collected information can be configured through generic monitoring policy models.
OpenPMF™: 5. Update technical security policies automatically

MDS updates technical security policies automatically when systems change. No need to manually update technical security policies. This unique feature makes policy management and implementation manageable for today’s rapidly evolving interconnected applications (e.g. agile SOA w. BPM and clouds).
OpenPMF™: 6. Verify compliance/accreditation automatically

This MDS feature automatically produces supporting evidence that the enforced security rules match with accreditation/compliance policy models & security policy models. It helps shorten accreditation/re-accreditation time and reduce cost (esp. for agile IT landscapes such as SOAs)
Integration

OpenPMF is standards-based (incl. Ecore/MOF, XMI, XACML, ABAC), award-winning, and patent-pending.

OpenPMF Components

- A model-driven policy authoring tool,
- A model-driven rule generation tool,
- An attribute-based authorization policy server,
- Policy decision/enforcement points,
- A model-driven compliance/accreditation evidence generation tool

The OpenPMF Solution is customizable for your particular business and IT landscape. We currently offer pre-developed integration and support for the following technologies:

- XACML Authorization Management
- Eclipse IDE & modeling framework
- BPMN business processes: Intalio BPMS
- SOA web app server: BEA Weblogic, Glassfish, Axis2/Tomcat
- Data Distribution Service: RTI DDS
- CORBA Components: Qedo CCM
- CORBA MICO C++ CORBA
- CORBA: JacORB Java CORBA
- Message-oriented middleware: XMLBlaster
- Fraunhofer FOKUS AD4 CCM MDA toolchain
- Firewalls: IIOP ObjectWall ('network PEP')
- Proma Raven NIDS
- Public Key Infrastructure (PKI): X.509
- Privilege Management (PMI): OMG ATLAS
- Directory Services: LDAP
- Databases: Secerno (under dev.)
- Databases: PostgreSQL (under dev.)
- Other technologies: supported on demand

info@objectsecurity.com
www.objectsecurity.com
OpenPMF™ Cloudα
Policy as a Service
Conclusion

- **ObjectSecurity**: leader in model-driven security (MDS) policy automation (esp. for access control)

- **Problem**: Security policies are often:
  - either unmanageable, e.g. ABAC etc. or not good enough, e.g. IBAC/RBAC

- **Solution**: Model-driven security:
  - Automatically generate technical rules from human-intuitive, “undistorted” models
  - Automatically update technical rules when IT landscapes change
  - Automatically generate compliance/accreditation evidence

- **ObjectSecurity OpenPMF™**: leading, award-winning MDS product
  - (1) Reduces cost; (2) Improves security & accreditation/compliance; (3) Supports security for today's agile, interconnected applications (e.g. SOA/cloud).
Model-Driven Security Policy Automation

USA

ObjectSecurity LLC
1855 First Avenue, Suite 103
San Diego, CA 92101
USA
Tel. +1-650-515-3391
Fax +1-360-933-9591

EMEA

ObjectSecurity Ltd.
101 The Embarcadero, Suite 200
San Francisco, CA 94105
(please send postal mail to San Diego office)
St John's Innovation Centre
Cowley Road
Cambridge CB4 0WS
United Kingdom
Tel. +44 1223 420252
Fax +44 1223 420844

Questions?

Ulrich.Lang@objectsecurity.com
www.objectsecurity.com
info@objectsecurity.com

Object Security
Secure technology

info@objectsecurity.com
www.objectsecurity.com